PRODATIS®

The eBusiness Solution Company.

So gehen Beschäftigte mit „aufgedrängten Daten“ um

So gehen Beschäftigte mit „aufgedrängten Daten“ um

Will ein Unternehmen personenbezogene Daten erheben, erhält es oft Informationen, die über die abgefragten Daten hinausgehen. Denkbar ist auch, dass Kunden oder Mitarbeiter ungefragt personenbezogene Daten übermitteln. Was tun mit solchen Daten?

Von „aufgedrängten Daten“ spricht man, wenn betroffene Personen personenbezogene Daten übermitteln, ohne dass der Verantwortliche diese Informationen angefragt hat, oder wenn die Angaben, die eine betroffene Person macht, über die abgefragten Informationen hinausgehen. Beispielsweise füllen Mitarbeiter Freitextfelder mit personenbezogenen Daten aus. Oder Bewerber teilen ungefragt Erkrankungen mit oder schicken unaufgefordert ein Foto.

Vor dem Hintergrund des Grundsatzes der Datensparsamkeit, aber auch angesichts der Rechtsfolgen einer Datenverarbeitung, beispielsweise hinsichtlich etwaiger Informationspflichten, ist es für die Verantwortlichen wichtig, den Umgang mit einer solchen „aufgedrängten Verarbeitung“ zu regeln. Und darüber hinaus gilt es, die Beschäftigten dafür zu sensibilisieren, wie sie mit solchen Daten korrekt umzugehen haben.

Ist die DSGVO bei aufgedrängten Daten anwendbar?

Damit das Datenschutzrecht mit all seinen Rechtsfolgen Anwendung findet, ist ein Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 Datenschutz-Grundverordnung (DSGVO) nötig. Darunter fällt auch die Erhebung personenbezogener Daten.
Hierunter versteht die DSGVO ein erstmaliges und zielgerichtetes Zugreifen auf die personenbezogenen Daten einer betroffenen Person. Es ist also ein aktives Tun des Verantwortlichen erforderlich.

Ein bloßes „Mitbekommen“ genügt nicht

An einem aktiven Tun seitens des Empfängers der Daten fehlt es jedoch zunächst bei der aufgedrängten Verarbeitung. Denn in diesen Fällen erhält der Verantwortlichen ohne sein Zutun diese personenbezogenen Daten. Auch wenn den aufgedrängten Daten eine Abfrage personenbezogener Daten vorausging, so wollte der Empfänger diese Angaben nicht erhalten.

WICHTIG

Ein bloßes „Mitbekommen“ personenbezogener Daten stellt nach Auffassung der Datenschutzaufsichtsbehörden noch keinen Datenerhebungsvorgang dar.

Das sieht z.B. die Saarländische Beauftragte für Datenschutz und Informationsfreiheit in ihrem Tätigkeitsbericht so (vorgelegt am 11. März 2020).

Auch Informationen, die Kunden oder Mitarbeiter dem Empfänger aufgedrängt haben, fallen dementsprechend nicht unter den Begriff des Erhebens. Folglich lösen aufgedrängte Daten zunächst keine datenschutzrechtlichen Folgen aus. Der Empfänger muss also z.B. keine Informationspflichten gegenüber dem Betroffenen erfüllen.

Aufgedrängte Daten sofort löschen, wenn möglich!

Damit Verantwortliche bei aufgedrängten Daten nicht den Verarbeitungsbegriff erfüllen und die Rechtsfolgen der dann anzuwendenden datenschutzrechtlichen Regelungen auslösen, müssen sie sämtliche Daten, die ohne Grund an das Unternehmen oder die Behörde übermittelt wurden, unverzüglich löschen bzw. vernichten.

Bietet sich eine Löschung des fraglichen Datensatzes nicht an, weil ein Bewerber ihn im Rahmen von zusammenhängenden Bewerbungsunterlagen übermittelt hat, ist es denkbar, das aufgedrängte Datum zu schwärzen. Hierbei ist es noch nicht erheblich, dass der Mitarbeitende diese Daten sieht – insoweit ist eine reine Kenntnis unschädlich, und es findet kein Verarbeitungsvorgang statt.

PRAXIS-TIPP

Die Beschäftigten müssen also wissen: Sobald sie personenbezogene Daten erhalten, die über das geforderte Maß hinausgehen, müssen sie diese Informationen möglichst gleich löschen. Lässt sich das nicht umsetzen, müssen sie die betreffenden personenbezogenen Daten schwärzen.

Verarbeitung der aufgedrängten personenbezogenen Daten

Landen diese Daten jedoch in einer strukturierten Form in den eigenen Systemen oder Archiven, kommen die Regelungen der DSGVO zum Tragen. Möchte der Verantwortliche die Informationen nun doch verarbeiten oder ist es systemseitig nicht möglich, ein separates Datum zu löschen, stellt sich zunächst die Frage nach der Rechtsgrundlage.

Rechtsgrundlage?

Gemäß Art. 6 Abs. 1 DSGVO dürfen Verantwortliche und Auftragsverarbeiter personenbezogene Daten nur verarbeiten, wenn hierfür eine gesetzliche Erlaubnis besteht.

Insbesondere bei Daten besonderer Kategorien wie Gesundheitsdaten, Angaben zur Religion etc. kann die Rechtsgrundlage eine Herausforderung darstellen. Denn für eine Verarbeitung dieser Daten ist im Regelfall eine Einwilligung des Betroffenen erforderlich.

Dazu kann es bereits kommen, wenn ein Bewerber ungefragt ein Bewerbungsfoto mitschickt, das ihn als Brillenträger erkennbar werden lässt. Auch hierbei handelt es sich um ein Gesundheitsdatum.

Rechtsfolgen einer (aufgedrängten) Verarbeitung

Grundsätzlich finden sämtliche Vorschriften Anwendung, die auch für eine „reguläre" Verarbeitung gelten. Soll also ein aufgedrängtes Gesundheitsdatum verarbeitet werden und findet keine Ausnahme von Art. 9 Abs. 2 Buchst. b–j, Abs. 3 und 4 DSGVO Anwendung, ist unmittelbar eine Einwilligung des Betroffenen nötig.

Machen Sie die Beschäftigten darauf aufmerksam, dass sie das Datum löschen müssen, wenn die betroffene Person nicht einwilligt und kein anderer Gestattungsgrund vorliegt.

Informationspflichten

Von praktischer Relevanz sind des Weiteren v.a. die Informationspflichten nach Art. 13 und 14 DSGVO. Kommt es also zu einer Speicherung etwa in einem Customer-Relationship-Management-(CRM-)System des Verantwortlichen, muss eine entsprechende Mitteilung an den Betroffenen erfolgen.

Empfehlen Sie, eine E-Mail mit einer Verlinkung zu den Datenschutzhinweisen zu verschicken, die über die Verarbeitung aufklären, oder die betroffene Person über eine gesonderte Nachricht über die konkrete Verarbeitungssituation zu informieren.

Was müssen Unternehmen und öffentliche Einrichtungen beachten?

Sensibilisieren Sie die Kolleginnen und Kollegen dafür, darauf zu achten, dass Abfragemasken und -bögen möglichst klar und verständlich sind. So ist für den Betroffenen erkennbar, welche personenbezogenen Daten anzugeben sind. Das minimiert Eintragungen an den falschen Stellen bzw. unnötige Antworten.

Daneben sollten die Masken und Bögen entsprechend dem Grundsatz von „privacy by design" nach Art. 25 DSGVO so gestaltet sein, dass sie nur Daten abfragen, die für den bestimmten Zweck erforderlich sind.

Für Fälle, in denen ohne einen vorherigen Kontakt personenbezogene Daten an ein Unternehmen übermittelt werden, ist es ebenfalls wichtig, Prozesse zu schaffen. Das kann neben einer angeordneten Löschung der Daten auch die Schulung des Personals, das diese Daten unter Umständen empfängt, umfassen.

Das sollten die Kolleginnen und Kollegen aus einer Schulung mitnehmen

1. Durch entsprechend gestaltete Eingabemasken möglichst verhindern, dass es überhaupt zu aufgedrängten personenbezogenen Daten kommt.
2. Sind sie trotzdem da: Daten möglichst löschen oder schwärzen
3. Ist das nicht möglich, greifen die Regelungen der DSGVO
4. Damit muss für jede Verarbeitung eine Rechtsgrundlage vorhanden sein. In vielen Fällen wird es auf eine Einwilligung hinauslaufen.
5. Ist das der Fall, ist zu prüfen und festzulegen, für welchen Zweck diese Daten tatsächlich notwendig sind.
6. Außerdem: Datensparsamkeit beachten! Es sollten nur solche Daten verarbeitet werden, die für den vorab definierten Zweck erforderlich sind.
7. Darüber hinaus ist die betroffene Person über diese Verarbeitung zu informieren.

Quelle:
www.datenschutz-praxis.de